



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,713	10/19/2000	Kunihiko Miyazaki	16869P-011500	7398

20350 7590 08/09/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

HOFFMAN, BRANDON S

ART UNIT PAPER NUMBER

2136

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/693,713

Applicant(s)

MIYAZAKI ET AL.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 June 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 7,9-12,21,23-26,30 and 34-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 7,9-12,21,23-26,30 and 34-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 7, 9-12, 21, 23-26, 30, and 34-38 are pending in this office action, claim 38 is newly added.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
3. Claims 34 and 36 are rejected as being dependent upon a canceled claim, namely, claims 1 and 13.

Claim Rejections - 35 USC § 103

4. Claims 7, 9-12, 21, 23-26, 30, 35, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. Patent No. 5,659,616) in view of Schneier et al. (U.S. Patent No. 5,956,404).

Regarding claims 7, 21, and 30, Sudia teaches a digital signature verifying method/apparatus/computer program, comprising:

- Accepting a message (fig. 9, ref. num 901/921);
- Acquiring a log list of a digital signer (fig. 9A, users smart card and col. 18, lines 8-22); and

- Checking whether log data of said digital-signature-attached message is registered in said log list (col. 18, lines 8-22),
- And if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer (fig. 9, ref. num 921),
- Wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer (col. 11, lines 12-41).

Sudia does not specifically teach the accepting is of a digital-signature-attached message that is to be verified.

Schneier et al. teaches accepting a digital-signature-attached message (col. 5, lines 35-41), wherein said digital-signature-attached message **which** may have been distributed by said digital signer is to be verified (col. 11, lines 45-48).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accepting a digital-signature-attached message, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified, as taught by Schneier et al., with the method/apparatus/

computer program of Sudia. It would have been obvious for such modifications because a digital-signature-attached message provides a strong audit trail; a strong audit trail provides an indisputable list of actions to verify all events that took place.

Regarding claims 9 and 23, the combination of Sudia in view of Schneier et al. teaches:

- Wherein said digital-signature-attached message further comprises data from a previously signed message (see col. 11, lines 30-64 of Schneier et al.),
- Said method further comprising checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer (see col. 11, lines 12-41 of Sudia).

Regarding claims 10 and 24, the combination of Sudia in view of Schneier et al. teaches said method further comprising checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered (see col. 11, lines 45-48 of Schneier et al.).

Regarding claims 11 and 25, the combination of Sudia in view of Schneier et al. teaches:

- Wherein said log data further comprises a distribution destination (see col. 6, lines 27-29 of Schneier et al.),
- Said method further comprising acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list (see col. 11, lines 30-42 of Schneier et al.), and
- Checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered (see col. 11, lines 44-50 of Schneier et al.).

Regarding claims 12 and 26, the combination of Sudia in view of Schneier et al. teaches:

- Wherein said digital-signature-attached message further comprises a timestamp created using a second secret key (see col. 12, lines 41-48 of Schneier et al.),
- Said method further comprising acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message (see col. 12, line 65 through col. 13, line 1 of Schneier et al.); and

- Checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message (see col. 12, lines 49-59 of Schneier et al.),
- And if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature (see col. 12, line 59-65 of Schneier et al.).

Regarding claims 35 and 37, the combination of Sudia in view of Schneier et al. teaches wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message (see col. 6, line 65 through col. 7, line 15 of Schneier et al.).

Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,956,404), hereinafter referred to as '404, in view of Schneier et al. (U.S. Patent No. 5,978,475), hereinafter referred to as '475.

Regarding claim 38, '404 teaches a digital signing system, said system comprising:

- A digital signing apparatus (col. 5, lines 7-34);
- A timestamp issuing apparatus (col. 10, lines 30-37); and
- A digital signature verifying apparatus (col. 12, lines 49-59),

- Said digital signing apparatus comprising a processor and a communication interface (col. 5, lines 22-28), wherein said processor applies a first secret key to a message or to its hash value to generate a digital signature (col. 5, lines 7-9), said processor transmits said digital signature to said timestamp issuing apparatus by said communication interface and acquires a timestamp in response (col. 10, lines 44-50), and said processor attaches the acquired timestamp to said message to create a digital-signature-attached message (col. 12, lines 45-47 and fig. 3, ref. num 285),
- Said timestamp issuing apparatus comprising a processor and a communication interface (col. 5, lines 22-28), wherein said processor generates a timestamp by applying a second secret key to data which includes the digital signature sent by said digital signing apparatus, and a reception time of the digital signature (col. 10, lines 30-34), and said processor transmits said timestamp to said digital signing apparatus (col. 10, lines 34-37), and thereupon
- Said processor checks whether data and time indicated by the time data exceeds expiration date and time assigned at said digital signing apparatus (col. 12, lines 49-59), and when the date and time indicated by the time data does not exceed the expiration date and time, said processor authenticates the validity of the said digital signature (col. 12, lines 59-65).

'404 does not teach accepting a digital-signature-attached message to be verified, acquiring a digital signature and time data, and authenticating whether said

digital signature has been generated for the message included in said digital-signature-attached message.

'475 teaches said digital signature verifying apparatus comprising a processor interconnected with an input device (fig. 1B, ref. num 110 to 180), wherein said input device accepts a digital-signature-attached message to be verified (col. 13, lines 15-33), and said processor acquires a digital signature and time data by applying a public key paired with the secret key of the timestamp apparatus to the timestamp included in said digital-signature-attached message (col. 15, lines 1-8), and thereupon said processor authenticates whether said digital signature included in said digital-signature-attached message has been generated for the message included in said digital-signature-attached message, using said digital signature, the message included in said digital-signature-attached message, and a public key paired with the secret key of the digital signing apparatus (col. 15, lines 1-8).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accepting a digital-signature-attached message to be verified, acquiring a digital signature and time data, and authenticating whether said digital signature has been generated for the message included in said digital-signature-attached message, as taught by '475, with the system of '404. It would have been obvious for such modifications because the system provides a verifying machine a secure audit log for a trusted machine and an un-trusted machine. By using a public


Art Unit: 2136


key and a corresponding secret key, the audit log can only be viewed by its intended recipient.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


BH


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100